Available online at www.sciencedirect.com

SciVerse ScienceDirect

Procedia Engineering 29 (2012) 123 – 127

Procedia Engineering

www.elsevier.com/locate/procedia

2012 International Workshop on Information and Electronics Engineering (IWIEE)

Design of Software to Search ASP Web Shell

Xu Mingkun*, Chen Xi, Hu Yan

Beijing University of Posts and Telecommunications,Beijing, 100876, P.R. China

Abstract

ASP Web Shell is a kind of ASP Trojan horse program, it has no obvious distinction with normal ASP programs. This is the reason why ASP WebShell has become the main approach to attack websites. In recent years ASP WebShell has applied varied technique to hide its characteristics to escape from killing, and techniques of WebShell finding and anti-finding contest further. After discussing the principle of ASP WebShell, this project makes focal points on the latest technology of anti-killing webshell, and introduces a program to search all kinds of WebShells automatically.

Keyword: ASP WebShell ; anti-killing Trojan horse; anti-virus software

1. Introduction

ASP WebShell is a kind of ASP Trojan horse programs [1]. It and other ASP programs have no essential differences. It can run in the same environment where ASP can run. This is the reason why ASP WebShell has become the main approach to attack websites. Finding WebShell is an important requirement to secure ASP Web site

The features of early Trojan horses are obvious, so to discover Trojan horse is easy for website administrator and anti-virus software. In recent years ASP Trojan horses have applied varied technique to hide its characteristic, and techniques of Webshell finding and anti-killing contest further more. This article discusses ASP WebShell 's principle, focuses on how to find out anti-finding Webshells.

* * Corresponding author.
E-mail address: henry7120@hotmail.com.

doi:10.1016/j.proeng.2011.12.680

2. The principle of ASP WebShell and method to discover it

To look for ASP WebShell, we first need to study the principle and characteristic of ASP WebShell.

2.1. The characteristics of ASP WebShell to call component

The main function of the WebShell, is to change webpage files and database. ASP WebShell usually call file and database components, combined with other techniques to revise content of webpage and control website [2].

Most ASP WebShell will call FileSystemObject component, commonly known as FSO. FSO component provides powerful ability to read, create, modify, delete, rename files on target website， so FSO Trojan horse may be seriously destructive . Webshell also often call other powerful components, such as WScript.Shell, Adodb.stream，Shell.applicaiton components etc. All webpages that call to these components should be examined carefully.

2.2. characteristics of one statement Trojan Horse

One statement Trojan horse [3] has no independent ability to control website, but if it is used together with client code, it can control website. It usually has the following form:

<%eval request("MH")%>;

<%execute request("MH")%>

To handle this kind of Trojan horses: find out eval and execute statements.

2.3. The Techniques of anti-finding Trojan Horse and method to discover it

The principle for anti-finding Trojan to revise webpage remains the same with ordinary Trojan horse, however, by modifying its own characteristics, anti-finding Trojan tries to escape from anti-virus software or website administrator.

2.4. Call components by CLSID [2]

In order to avoid explicit call to components, which will alert website administrator, Trojan often calls components through CLSID, commonly involved components are:

WScript.Shell (classid:72C24DD5-D70A-438B-8A42-98424B88AFB8)；

WScript.Network (classid:093FF999-1EA0-4079-9525-9614C3504B74；

FileSystemObject(classid:0D43FE01-F093-11CF-8940-00A0C9054228)；

Adodb.stream (classid:00000566-0000-0010-8000- 00AA006D2EA4).

To handle this kind of Trojan: look for common CLSID.

2.5. Case conversion

To change case of Trojan horse code, Trojan can escape from some anti-virus software.

To handle this kind of horse, just ignore case when compare webpage code with Trojan horse feature.

2.6. Utilizing connecting symbol to hide Trojan feature

For example, statement Set hh = Server.CreateObject

("Scripting.FileSystemObject") can be replaced by following statement: Set hh=Server.CreateObject ("Scrip"+"ting.file"+"systemobject") or Set hh = Server.CreateObject ("Scrip" & "" & "ting.file systemobject").Execution result is the same, but it can escape the anti-virus software [4].

To deal with this kind of Trojan: replacing connecting symbols first, and then look for horse feature.

Trojan horse may also insert empty variable to avoid being discovered: Set hh=Server.CreateObject ("Scrip"&"ting.file"&qsd&"systemobject") where qsd is an empty variable.

To deal with this kind of Trojan: directly find out CreateObject statement.

2.7. Method to use picture or combine files

ASP page can use <!--include file = "xxx/2.gif"--> statement to call Trojan horse embedded in picture [5], where xxx /2.gif is the picture's location on web server. Hacker can connect the ASP mentioned above.

How to handle it: update security patches; find out ASP file which calls picture.

Trojan horse may segment its code into several ASP files to hide feature, then use #include statement to combine these files, in order to escape from anti-virus software.

How to handle it: abnormal #include statement is feature of Trojan.

2.8. Add useless characters to hide Trojan feature

Any comment/*.. */,// in the end of a line, or NULL, inserted in webpage, will not affect the execution of Trojan horse, but may interfere anti-virus software [6].

How to handle it: scan web pages twice, first remove all the comments and NULL characters to generate a intermediate file, second time scan intermediate file to look for Trojan feature.

2.9. Encode, US_ASCII and VBS encryption method

Commonly used is the Microsoft source code encryption tools ， Script Encoder，which lets horse to avoid being found. US_ASCII encryption method is to set 1 on the utmost bit of each character, so characters garble like Chinese codes ,with many % symbol in webpage [6]. There are some encryption software, for example, tool to merge the database file and Webpage, also can make web code unreadable, or convert JS code to VBS code. Though these cryptographic Trojan horses hide their Trojan features, but the garbled characters themselves become the new features. Rich garbled characters or peculiar VBS statement can be found out for administrator to examine.

2.10. The escape functions and escapes encryption method

JS language has an escape function which can let the page code hard to be recognized. But this kind of page code requires eval( ) function to decrypt. In JS, the escaped character can use octal or hexadecimal digit script code [6]. eval( ) function is called to interpret escaped characters.

How to handle escape encryption: find out escape, eval( ), document.write ( ) function [4].

2.11. Associative array method

JavaScript can deal with object as associative array, e.g. OBJECT.ATTRIBUTE and OBJECT ["ATTRIBUTE"] have the same meaning [4]. OBJECT object constitutes an associative array. On the latter's character string, various character encryption method can be applied to revise Trojan features.

How to handle this kind of encryption: the same with section 2.10.

2.12. Custom encryption technology

First write a encryption function, such as the string reverse function, encrypt the original WebShell as a string, the encrypted string and the corresponding decryption function constitute a new WebShell, which can be executed through eval( ), execute( ) or document. write( ) function. Because this kind of Trojan can change any Trojan signatures, it is possible to escape from any antivirus software theoretically. But writing dedicated encryption and decryption function needs complicated technique , even if encryption is successful, by restricting file uploading and user permissions, etc, this kind of Trojan can do nothing, so custom encryption method is seldom to be found [4].

How to handle this kind of encryption: the same with section 2.10.

3. WebShell finding software algorithm and its run result

3.1. Software Algorithm

This project develops a WebShell search software with c++ [2], it recognizes features mentioned above. Feature library is flexible; certain features can be added or deleted from the library according to administrator's requirement. The software recursively looks for WebShell features inside each file in any website directory tree; any suspicious file will be selected for administrator to examine further.

3.2. Software Run Resultm

When testing the software, take typical dozens of WebShells as specimen, the software is able to detect all the suspicious files for administrator. All the real webshell can be checked out through administrator's examination. And this software has been deployed in actual website which users can upload files, in the past year is never webshell able to escape its search, which proves that the search algorithm is accurately and effectively. But this result does not guarantee that detection rate is 100% in future, because there may be specimen not known. If other webshell feature is got, it can be added into webshell feature library.

4. Conclusions

The software's result to discover webshell is satisfactory, but it can not substitute other security measures .Combination of IIS and operating system security patches [7], database injection prevention and other security measures, will make website more secure and reliable.

Webshell has no absolute distinction with normal administration webpages , they are all belong to remote control software. If it is used to undermine website subjectively, it is Trojan horse; If it is used to manage website subjective, it is normal management software. In theory, only administrator can judge whether a remote management webpage has wicked behavior [8].

There are some encryption webshells which has no obvious characteristic to search, but when it is scheduled into memory for execution, the encrypted webshell will restore to original code which can be easily identified [4]. This software has no such memory webshell search function. And memory webshell

search involves a lot of realtime tracking and anti-tracking techniques, which need additional analyze elsewhere.

The search method of this software can be extended to all other kind of websites, such as PHP, JSP, ASP.NET websites, just webshell feature library and software operating environment need to change. In terms of target classification, the likelihood in the Bayesian updating procedure can be naturally and better explained as a possibility than as a probability interpretation. With an accurately defined feature mapping based on this possibility viewpoint, the proposed Bayesian classifier outperforms the conventional Bayesian classifier and provides precise classification results.

Acknowledgements

Youth Innovation Foundation of Beijing University of Posts and Telecommunications: Portal Site Specific Project.

References

[1] Baidu Corporation,Webshell , http://baike.baidu.com/view/53110.htm

[2] Microsoft Corporation，Visual Studio 2008,MSDN , Electronic Document.

[3] Hu Dong,Webpage Trojan Technology, http://wenku.baidu.com/view/0a2336d049649b6648d747a2.html

[4] Ren Fei, Web Trojan Defense Practics. PUBLISHING HOUSE OF ELECTRONICS

[5] The Hiding of Webshell, http://www.mbsky.com/InfoView/Article_5381.html

[6] Xiao Yao, Large and Medium-Sized Network Intrusion Cases Research. Publishing House Of Electronics Industry.October 2010.pp.301-310

[7] Marty Jost,IIS Security2002 by McGraw-Hill,.pp.249-270

[8] Markus Jakobsson, Crimeware: Understanding New Attacks and Defenses, Publisher Addison-Wesley Professional.Pub.April, 2008.pp.9-27(in Chinese)